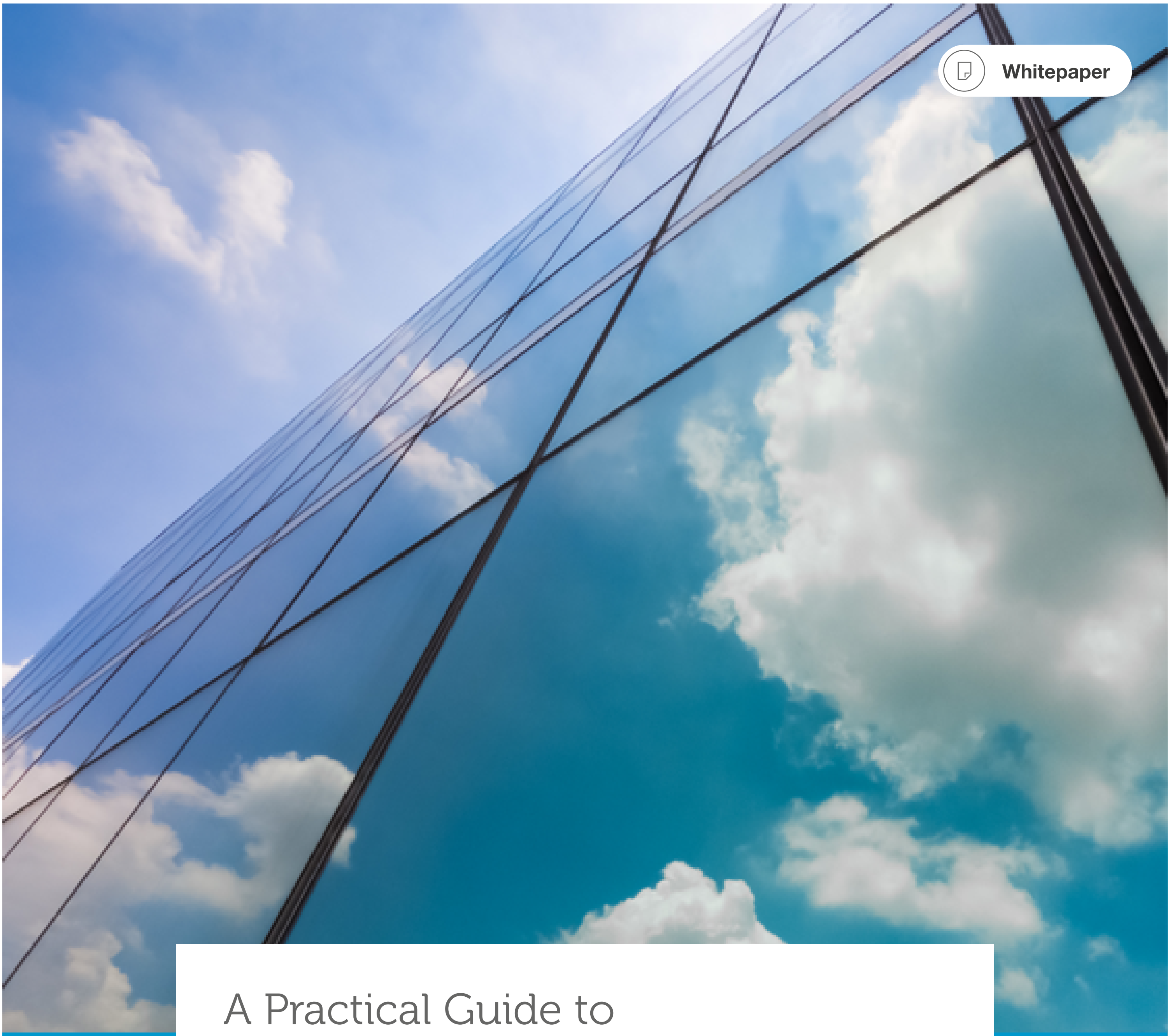
interxion™

Whitepaper



A Practical Guide to Cloud Onboarding

How to prepare your application workloads

INTRODUCTION

No IT department wants to launch itself into a cloud migration project without feeling confident that it can ultimately deliver a smooth, trouble-free switchover to the cloud environment. Papers and articles selling the benefits of cloud computing may gloss over the whole issue of onboarding, as if 'forklifting' applications into a cloud environment is as easy as flicking a switch (as long as you use their solution). Clearly it isn't, even for applications regarded as being relatively 'easy' to migrate to a cloud environment.

The complexity of onboarding is a big part of why enterprises are hesitant about cloud projects, despite being sold on the benefits of cloud delivery. A lot rides on getting the migration right.

Why consider cloud migration?

So, why take the plunge at all? Cloud migration might make sense for a number of reasons, including:

- **Business growth**. Many businesses choose to deploy applications from the cloud as a faster route to new markets, both nationally and internationally. Connectivity is a crucial success factor here, because customers worldwide expect the highest quality of digital experiences. Applications deployed closer to the end user can deliver low-latency, reliable connectivity, and a choice of diverse local connectivity providers gives you full control over how you serve customers in each new market.

- **IT agility**. A cloud-based IT environment allows you to create new products faster and respond more quickly to customer demands. By deploying applications in the cloud, closer to the end user, you can scale resources to meet temporary surges in demand, serving that need faster than if you were to deploy from a local data centre.

- **Strategic flexibility**. Applications deployed in the cloud can also help reduce capital and operating expenses. In fact, our 2017 research report “The Digital Enterprise” found that cost is the most common reason why companies choose to change how their IT is housed. Cloud also offers the flexibility to choose when and how you expand, making it a valuable strategic asset.

What do we mean by 'onboarding'?

In the context of migration to a cloud environment, 'onboarding' refers to the deployment of applications, data or both to the chosen cloud infrastructure (public, private or hybrid). It's essentially the final stage of the migration process: the equivalent of the transition from one network to another in a network migration project.

As with a network migration project, this final stage of the process is supposed to happen smoothly and quickly. If everything has been properly prepared beforehand, there's no reason why it shouldn't. Successful onboarding is all about prior planning and preparation.

Who this paper is for

Another Interxion whitepaper, **“The Enterprise Guide to Cloud Migration,”** explores Gartner’s five key migration paths: (1) rehost on IaaS, (2) refactor for PaaS, (3) revise for IaaS or PaaS, (4) rebuild on PaaS, or (5) replace with SaaS.

In this paper, we’ll focus on paths 1 and 3. These are migrations that 'forklift' applications (or virtual machines and the applications that run on them) into a virtual private cloud or public cloud environment without the need for major refactoring or rebuilding. We lay out some key considerations for IT decision-makers who want some answers to the 'how' of application onboarding.

Some of what we’ll cover will be relevant to paths 2 and 4, but the process of refactoring or rebuilding an enterprise application for cloud migration is not our focus here. Nor is path 5, where an existing application is being replaced rather than migrated (although in the SaaS scenario some onboarding may still be required – data may need to be migrated, for example).

The first part of the paper explains why application onboarding may seem to be a challenge and introduces the key concepts and considerations. The second part introduces the steps of onboarding and the three critical areas of preparation that are necessary to ensure successful negotiation of those steps. We then cover these three success factors in more detail.

APPLICATION WORKLOADS AND IMPLICATIONS FOR ONBOARDING

When talking about cloud migration or onboarding, cloud service providers usually talk about 'application workloads' rather than just 'applications'. This is because applications don't operate in isolation, and the 'workload' concept captures the notion of all the work being done by a system when an application is running.

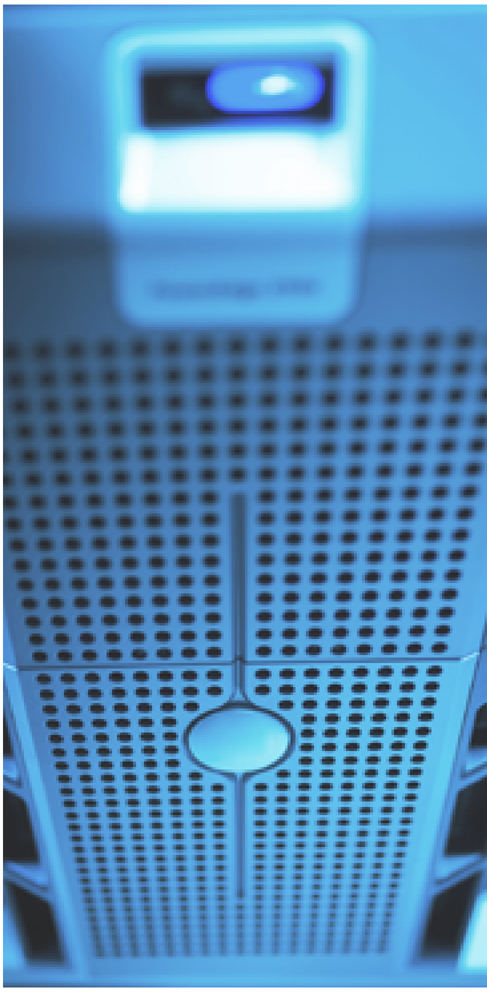
An application workload can therefore be thought of as a logical container that includes all of the components required for the proper performance of an application. It includes the processing power used directly by the application, the storage being read from and written to, the network connectivity being used, and the application's interactions with monitoring and management tools, security services, authentication services such as Active Directory, and other relevant services.

Complexities of enterprise application workloads

When you're migrating an application to a cloud environment, some of these elements won't be migrated with the application. For example, it's common for enterprises to maintain their Active Directory domain controller in-house while some of the applications it controls reside in a third-party cloud environment. Enterprise applications also usually interact with one another – a logistics system managing deliveries might be integrated with a CRM system, for example. In this regard, most enterprise application workloads are quite unlike the monolithic cloud applications of Facebook, Zynga or Netflix, which are essentially run as 'standalone' dedicated applications, separate from general business functions and running at a much larger scale than enterprise applications.

Cross-platform interactions are a big part of the complexity of enterprise application onboarding, even for workloads perceived as ‘cloud-friendly’. It's also one of the reasons that enterprises might start with private cloud deployments. Rightly or wrongly, enterprises may feel that in a private cloud environment they can control the cross-platform interactions of their cloud applications more easily than in a public cloud environment.

How many of your workloads are cloud-friendly?



It's hardly surprising that most enterprises choose to start their forays into cloud computing with application workloads that minimise the complexity of onboarding.

Examples include:

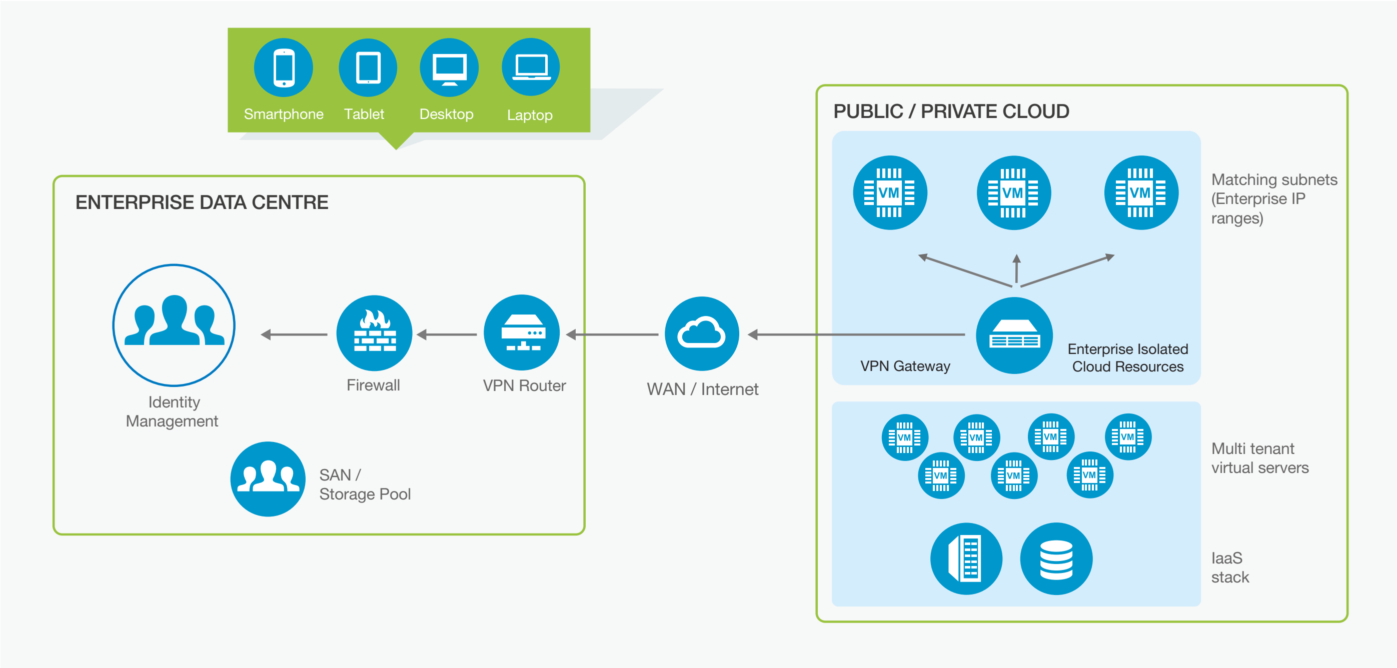
- **Test and development**: because applications under development are relatively 'standalone' in terms of level of interaction with other applications and services.
- **Collaboration and web applications**: because their native architecture is already compatible with running on loosely coupled computing and storage nodes.

For most enterprise applications, there's more work to do to prepare them for a cloud environment, because they're not natively designed for it. Whether off the shelf or made to order, they're designed to run on a single server or end-user machine, or on a cluster of front-end and application server nodes backed by a database. It's assumed that the application will be running on infrastructure designed for reliability, so hardware failure is taken to be an unlikely exception that requires special backup and disaster recovery procedures. This is quite different from a cloud environment that has built-in multi-site failover capabilities and is designed to 'expect' failure and respond to it by switching resources seamlessly.

Because of the work required to prepare traditional enterprise workloads for highly virtualised and standardised cloud environments, the most likely early candidates tend to be those already running in a virtualised environment.

Hybrid clouds are the new IT reality

Hybrid cloud environments – the integration of two or more different cloud environments – are emerging as the dominant model for enterprises. The integration of third-party cloud services with enterprise data-centre services is becoming common for several reasons:



- Cloud bursting (on-demand extension of the data centre to a cloud environment based on pre-defined policies and monitoring of loads, quality of service, and so on) is a way for enterprises to explore and trial cloud services when they have concerns about the security, stability or performance of the cloud environment.
- It's also a way to avoid investment in unused capacity to handle demand spikes. It's an attractive solution for enterprises facing periods of system overload and not wanting to over-provision their infrastructure.
- Enterprises occasionally have a need to migrate an executing workload from one environment to another, based on resource use and performance.
- As already discussed, cross-platform interactions are the reality for most enterprise applications, so unless and until enterprises are ready to operate everything in a single cloud environment, a hybrid model is the way forward.

Onboarding in a hybrid world

To make the most of hybrid cloud environments, enterprises need a well-understood and secure way to onboard workloads and then maintain two-way connectivity with their internal data centre. The key elements of the hybrid IT architecture are:

- The enterprise data centre (in house or located at a third-party data centre), which is assumed to be at least partly virtualised.
- The remote cloud environment: either a different enterprise data centre (private cloud), or the multi-tenant cloud platform of a cloud service provider (virtual private or public cloud). WAN connectivity between the two, usually via a secure internet VPN connection.
- End-user devices that access the applications hosted in the hybrid environment.

Typically, the external cloud resources are considered as a logical extension of the enterprise resources, with access only through the existing enterprise firewall. The enterprise's monitoring, management, trust and security policies and controls are applied to the cloud environment. Network isolation keeps enterprise workloads separate from those of other enterprises using the same multi-tenant cloud platform, and WAN traffic is generally encrypted. The latency introduced by both the WAN connectivity and the process of encryption and decryption may not be acceptable to certain workloads, which would then not make good candidates for cloud migration in the hybrid model.

Application onboarding: seven steps, three critical success factors

The actual process of onboarding ('forklifting' workloads) has seven relatively straightforward steps:

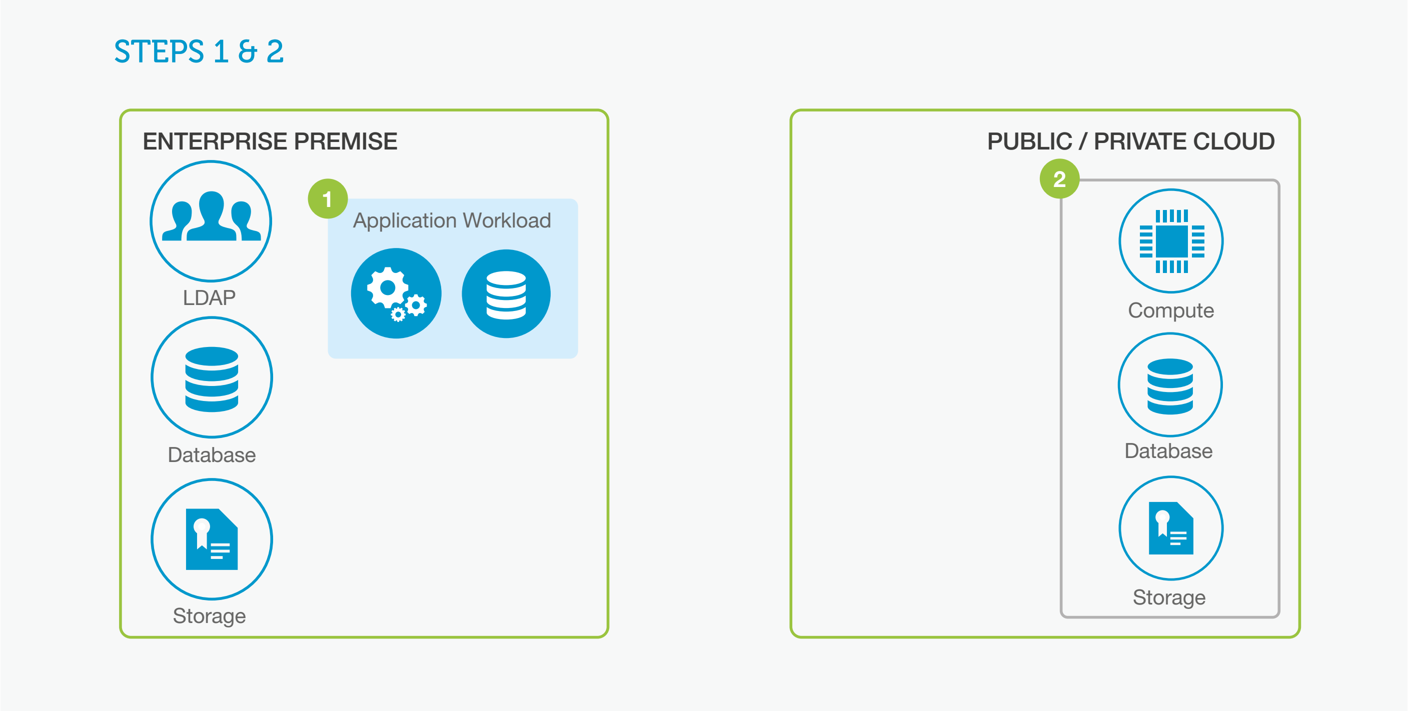
1. Defining the workload
2. Provisioning cloud resources
3. Establishing a connectivity bridge
4. Deploying the workload
5. Ensuring seamless two-way access
6. Testing and validating
7. Discontinuing the old service

Three critical success factors

As I've already pointed out, successful application onboarding is all about careful planning and preparation. There are three activities in preparing for onboarding that are critical to the ultimate success of the onboarding process:

1. Workload analysis: enables you to identify the most appropriate candidate workloads for cloud migration and understand their requirements for onboarding.
2. Getting the application cloud-ready: ensures that the application will perform as required on the target cloud architecture.
3. Choosing a cloud provider: determines the target cloud environment and may have implications for onboarding support.

The remainder of this paper looks at each of these in turn, though they can be considered as a set of activities running in parallel. Done with due care and thoroughness, they will put you in good stead to take the steps of application onboarding in your stride.

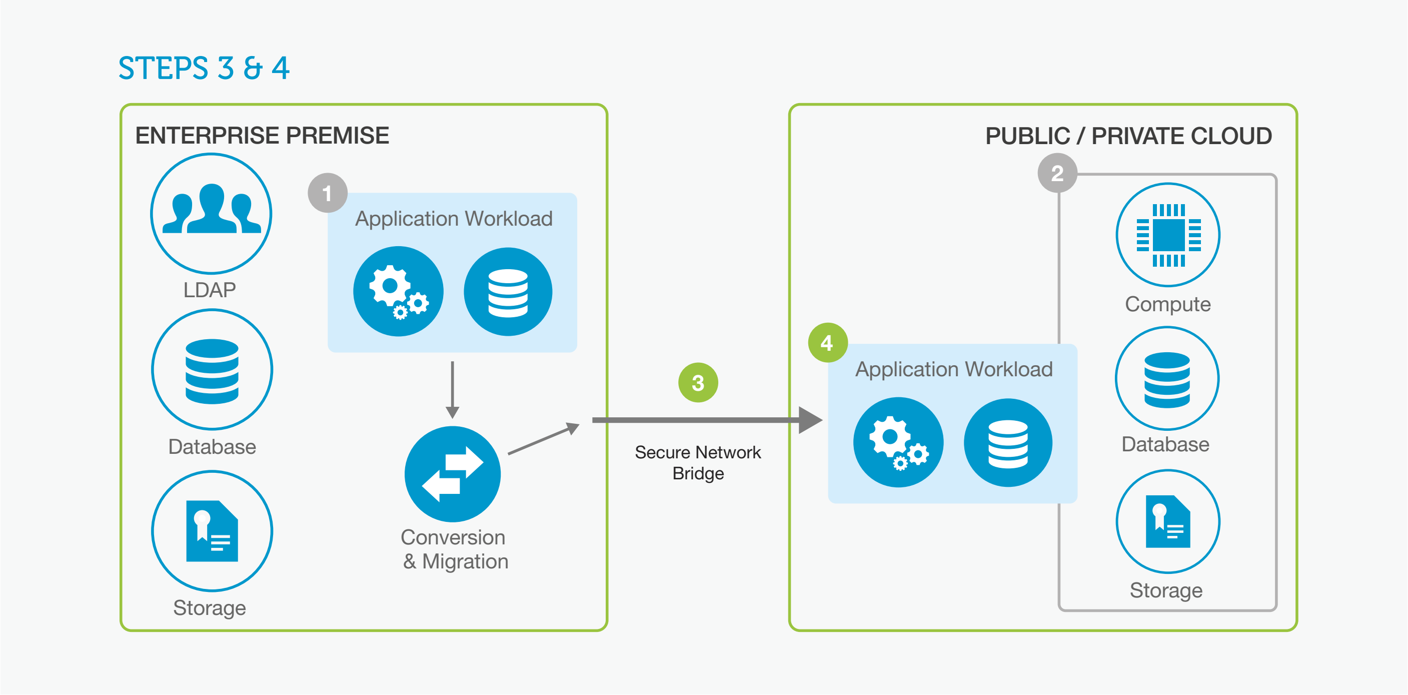


Step 1

Define the workload. The number and type of virtual machines required for migration will depend on the nature and scale of the workload, and the way it interacts with software and services not being migrated.

Step 2

Provision cloud resources. Service providers will have a self-service interface for the creation of accounts and purchase of the services that you need (e.g., servers, storage, network).

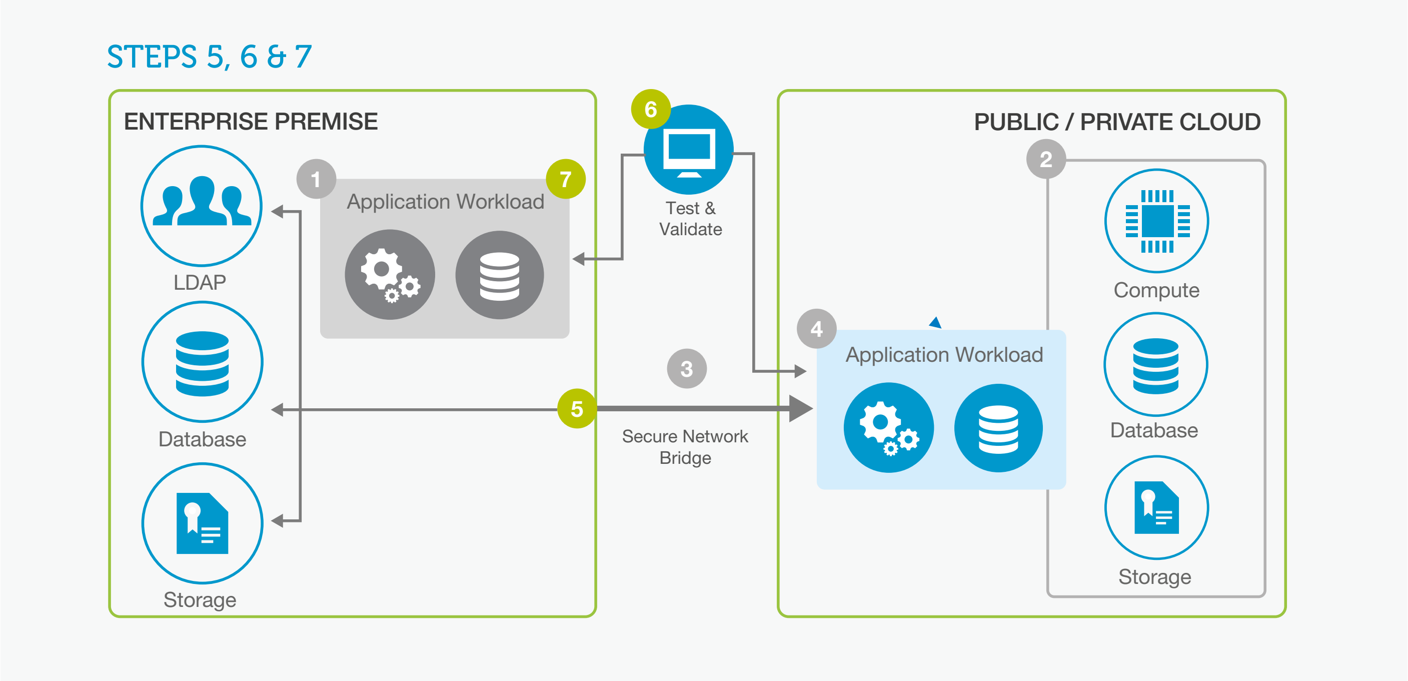


Step 3

Establish a connectivity bridge. Secure and transparent bi-directional connectivity, usually through an internet VPN, is required between your data centre and the cloud, both for the migration itself and for cross-platform application interactions after migration.

Step 4

Deploy the workload. With connectivity in place, virtual machines can be configured and connected to services remaining behind (such as Active Directory), followed by the transfer of the application and any associated databases, software and services being migrated.



Step 5

Ensure seamless two-way access. Smooth integration is required between the cloud workload and services not migrated, and you need to be able to monitor and manage the application as well as the cloud infrastructure.

Step 6

Test and validate. However well you've prepared and tested prior to deployment, there may be surprises. Has everything been transferred correctly? Do network, storage, compute and database configurations remain intact? Can you see and manage the cloud environment properly? Does your cloud backup process work?

Step 7

Discontinue the old service. When you're certain that everything is working well, you can give access to users and decommission the enterprise service.

SUCCESS FACTOR 1: WORKLOAD ANALYSIS

Because workloads differ in terms of their importance and cost to your organisation, a thorough workload analysis is critical to a successful onboarding process. A highly optimised application may be relatively easy to migrate to the cloud, but the move may offer little or no additional benefit for the effort. Choosing a workload that is both critical and complex to migrate is a big risk, but the potential cost savings or other benefits may outweigh the risk.

Workload analysis helps you identify and prioritise the best candidate workloads for migration, and should therefore combine business and technical factors. Workload analysis can also be used to inform decisions about the most appropriate cloud migration path (rehost on IaaS, refactor for PaaS, revise for IaaS or PaaS, rebuild on PaaS, or replace with SaaS) and the most appropriate cloud environment for applications (public, private, hybrid).

As well as helping you identify and prioritise candidate workloads for cloud migration, this kind of assessment will help you detail the requirements for onboarding of those applications that you do migrate. It will help you specify all the elements that make up the application workload, and the number and types of virtual machines (VMs) that need to be migrated.

What should you consider in your analysis? This workload assessment checklist will help:

Business impact	• How business-critical is the workload? Consider the answer against where you are on your cloud journey. • Where does the workload fit in the application lifecycle? What does that mean for its cloud environment requirements?
Business requirements	• Given the workload's business use, what are the implications for required service levels, transaction rates, response times, number of simultaneous users to be supported, or other relevant availability and performance-related measures? • What supporting service requirements does the workload have (e.g., in terms of backup, disaster recovery, monitoring) and what are the implications for cloud deployment? • Are there any specific security and compliance requirements (e.g. encryption, isolation, data sovereignty) and what does that mean for cloud deployment?
Application architecture	• Is the application architecture cloud-friendly in any way (e.g., is it horizontally scalable in the way that native cloud applications are, or only vertically scalable as traditional enterprise applications tend to be)? • If not, what's involved in refactoring the application for a cloud environment? • Are the time and cost acceptable when weighed against the benefits?
Computing resource and dependencies	• What OS, databases and application servers are being used and how hard are they to migrate to the cloud? • What are the CPU, memory, network and storage requirements and what will it cost to provide these in a cloud environment? • What other software supports the workload? What are the dependencies or integration touch points with other workloads?
Operational and support requirements	• How many hours/people are required to support the workload and what do they cost? • What are the costs of licensing? • What are the operational costs for space, power and cooling? • For these and other operational and support costs: will anything be saved by migration to a cloud environment?

SUCCESS FACTOR 2: GETTING THE APPLICATION READY FOR THE CLOUD

The next stage is getting the application and associated services ready for onboarding. This needs to be done in parallel with choosing a cloud service provider, because the environment you're moving to will be a big determiner of the work you need to do.

Preparing an application workload for 'forklifting' into a cloud environment will require virtualisation if the application is not already running in a virtualised environment. Associated databases may also need to be rationalised to work within, or with, the cloud environment. Complexities may arise at any level: from network and application components to the way provisioning, controls, or monitoring and management are going to work. As you tackle all of these, there are three fundamental characteristics to pay attention to:

- Scalability
- Resilience
- Security

The implications of scalability

The business case for cloud usually includes cost savings as a result of only paying for what you use. This is possible because cloud services can be scaled up on demand when you need to use more, and scaled down when you need to use less. But is the application workload that you're migrating suited to this model? Consider:

- **The dangers of upward scalability**. If an application is performing inefficiently in any way, it will use more resources than it should; and this can be costly in an environment where it's all too easy to provision more resources. To avoid scalability adding cost rather than saving you money, you need to identify and fix performance inefficiencies, for example by rooting out memory leaks or inefficient database queries. Where possible, isolate compute-intensive components in such a way that they can be scaled independently.
- **The requirements of downward scalability**. How effectively you can turn cloud resources off will depend on how easily you can isolate different application functions. To maximise the cost savings, you can make through downward scalability, break your workload into as many independently scalable components as possible.

Resilience

Resilience considerations are different in the cloud. Ideally you want workload components to be loosely coupled so that if one component fails, the others can continue to function. Depending on the criticality of your application, you may also need to ensure a greater degree of self-healing capability to ensure recovery from different types of failure at different levels: hardware, network and application. Safeguards could include process threads that resume on reboot, message queues that can reload the state of the system, and the use of a database rather than memory to write data to.

Testing, both before and at the end of the onboarding process, should include different types of failure scenarios to ensure appropriate resilience.

Security

Managing security in a cloud environment requires different approaches to respond to different vulnerabilities. In a multitenant environment, you'll typically want to take steps that you wouldn't otherwise, such as implementing encryption where you haven't before, or focusing on building security into applications rather than relying on traditional perimeter-based security controls. Both static and dynamic application security testing should be part of your application preparation.

SUCCESS FACTOR 3: CHOOSING THE RIGHT CLOUD SERVICE PROVIDER

When migrating applications to a cloud environment, the specific environment you choose and the services offered by your cloud service provider will determine the work you need to do and the help you can get in doing it. Ideally, therefore, you should choose your provider in parallel with analysing and preparing workloads for migration.

When considering cloud service providers, ask yourself:	
Migration	• Do they offer migration services that can help you avoid a steep learning curve and meet your budget and time constraints for onboarding? The large public cloud platforms tend not to, so you may need to engage with a systems integrator or other service provider that can provide the help you need
Application architecture	• Are their cloud architecture, standards and services suited to your workloads and management preferences?
Network architecture	• Is the provider's method of isolating your workloads from those of other customers appropriate to your needs and to your policies on network isolation?
Ease of Use	• How good are the provider's orchestration services? • What about the ease of self-service provisioning, management, and scalability?
Commercials and billing	• Do the commercial terms, cost model and billing options offer the flexibility that you need?
Ease of Use	• How good are the provider's orchestration services? • What about the ease of self-service provisioning, management, and scalability?
Performance guarantees	• Are the SLAs what you need and do you have clear visibility of performance, usage, costs and billing?
Security	• Is security built in and of the right standard? • Does the system allow different application workloads to talk to one another while maintaining security accreditations?
Business continuity	• Does the provider offer the resilience, business continuity and disaster recovery support that you need?
Governance	• Is there clear and appropriate service governance? • Does the provider support your compliance requirements?
Support	• What kind of support is offered and how is that charged?
Future	• Can the service provider help you with all of your likely future cloud requirements, not just your current ones? • And what about avoiding vendor lock-in: is the provider using open standards and APIs and do they have an offboarding process that is clearly covered in the contract? • What will be the cost of leaving?

Commercial models

When considering the cost of a cloud service, be careful to compare like with like. One of the benefits of the cloud model is cost transparency: it's very clear what you're paying when you consume IT resources. But when you're comparing the cost of a cloud service with the cost to provide the same service internally, the cloud service may look expensive if you haven't considered all of your internal costs. When you add up the bandwidth, connectivity, database, storage and compute costs of the cloud service, don't forget that the service provider's prices include all of the operational and support activities that you will no longer have to carry out. This is one reason why it's important for your workload analysis to be very thorough in attempting to capture all of the costs of running a workload in-house.

When discussing the implications of scalability earlier, I pointed out that if you can scale different workload elements independently, you can use cloud resources more efficiently. You may find that your ability to finetune scalability is affected by the way your cloud service provider packages its services, and you'll want to find a provider that matches your requirements in this regard. For example, consider the difference between these three typical models:

Pre-packaged tiers. Specified tiers come with a set amount of CPU core, RAM and disk space, with no room for custom configurations. It's simple, but you may pay for resources you don't need if demand for only one element requires you to go up a tier.

	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5	Tier 6
Core	1	1	2	4	6	8
RAM	512 MB	1 GB	2 GB	4 GB	6 GB	8 GB
Storage	20 GB	30 GB	40 GB	60 GB	90 GB	120 GB

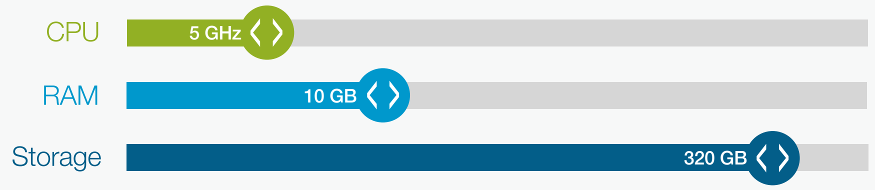
Source: Solar VPS (http://www.solarvps.com/linux-vps)

Per node/VM. This is a similar model to the tier approach, but the pre-defined packages (nodes) are more granular – allowing for more finetuning – and nodes often include a specified transfer amount (bandwidth), backup space and IP addresses in addition to CPU, RAM and storage. Customers buy the number of nodes they need for the period they need them.

	1 Node	2 Nodes	3 Nodes	4 Nodes	5 Nodes	6 Nodes
CPU	2.4 GHz	4.8 GHz	7.2 GHz	9.6 GHz	12.0 GHz	14.4
RAM	512 MB	1024 MB	1536MB	2048 MB	2560 MB	3072 MB
Storage	10 GB	20 GB	30 GB	40 GB	50 GB	60 GB
Transfer	3 TB	6 TB	9 TB	12 TB	15 TB	18 TB

Source: VPS.net (http://vps.net/cloud-servers)

Independently customisable. In this model, CPU, RAM and storage are decoupled and not forced to scale together. It's not as simple as the others to manage, but allows for very granular application of the pay-per-use model.



Source: CloudSigma (https://zrh.cloudsigma.com/ui/)

NEUTRAL DATA CENTRES ARE IDEAL FOR HYBRID CLOUDS AND APPLICATION ONBOARDING

Across Europe, enterprises rely on Interxion to host their mission-critical systems and data, drawn by the reliability, security and level of connectivity that our data centres provide. Interxion is a leader in driving data centre innovation, and we help enterprises take control of their cloud migration strategy so they can create the ideal IT environment on their terms, in their own way.

There are many reasons that businesses choose Interxion to colocate their cloud platforms and hybrid environments:

Connectivity

Having the right connectivity means being able to offer the best possible experience to your customers.

Interxion Cloud Connect offers a fast lane to the cloud through secure, high-performance private interconnections to multiple cloud service providers, including Amazon Web Services and Microsoft Azure. As one single physical connection built on carrier-grade hardware, Cloud Connect delivers low-latency and predictable bandwidth to enable faster speed to market, backed by a 99.999% SLA to ensure high redundancy.

We also offer an extensive choice of service providers within our carrier-neutral colocation data centres.

- More than 450 providers of cloud-related services, including both local and large, international cloud providers, and many systems integrators developing hybrid enterprise environments
- More than 700 connectivity providers: from Tier 1 carriers to mobile network providers, from ISPs to CDNs, and 21 Internet exchanges

Performance

Cloud services demand a high level of performance, reliability, security and scalability. We ensure performance through direct interconnection to the cloud platforms of your choice, including Microsoft Azure, Amazon Web Services, IBM Cloud and Oracle Cloud Infrastructure. Our award-winning data centres, designed for high-density cloud computing, are located in strategically important urban environments, which allows you to reach as many users as possible with the best quality performance.

Agility

With Interxion, you can scale capacity or adjust IT resources quickly to meet changing customer or operational requirements, both locally and internationally. With more than 45 data centres serving 13 European cities in 11 countries, Interxion is situated in Europe's leading business and residential centres, allowing you to reach more than 90 percent of Europe's broadband users.

Security

Security can be a major barrier to cloud migration. Interxion addresses this risk by meeting international security certifications, which reflect our commitment to protecting customer data. We also reduce IT risk by interconnecting to the cloud within the same data centre, providing secure connections backed by a 99.999% SLA. Interxion facilities also include multi-level physical security, 24/7 on-site security, surveillance cameras, private suites, and multiple layers of redundancy for power, cooling and fire-suppression.

Flexibility

Cloud migration with Interxion allows you to reach more customers and grow revenue potential without over-investing capital in expensive data centre build and management. You gain financial flexibility through a single connection to your cloud environment, which can reduce overall networking costs by 30 to 50 percent. Interxion also builds our data centres around “communities of interest,” which allow you to deploy your cloud near other business in your shared area of expertise. For example, a financial services business deploying applications in the same data centres as key business partners and associates cloud collaborate on operational and commercial tasks, unlocking new financial efficiencies and business opportunities.

Next steps

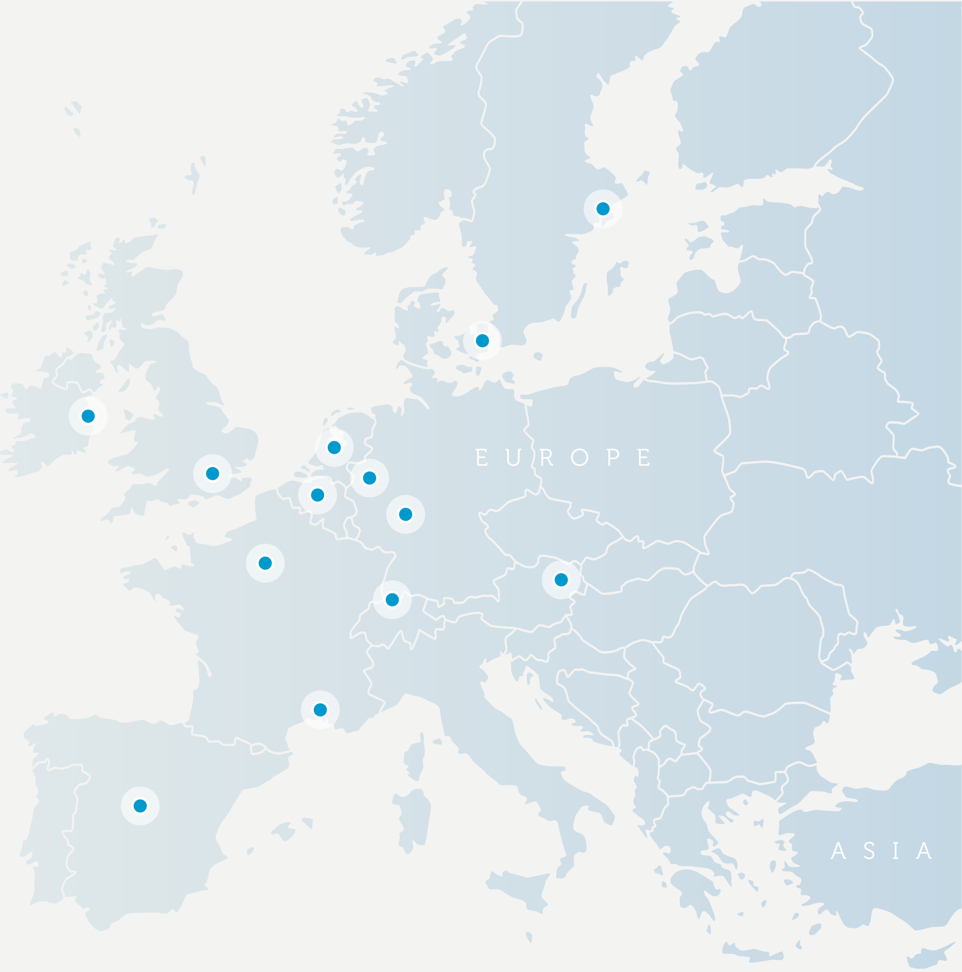
Please contact Interxion if you're looking for advice or assistance with a cloud migration project or if you have plans to build a hybrid cloud environment. As a neutral data centre provider, we can discuss your needs impartially and introduce you to the right suppliers and business partners across Europe.

About Interxion

Interxion (NYSE: INXN) is a leading provider of carrier and cloud-neutral colocation data centre services in Europe, serving a wide range of customers through over 45 data centres in 11 European countries. Interxion's uniformly designed, energy efficient data centres offer customers extensive security and uptime for their mission-critical applications.

With over 700 connectivity providers, 21 European Internet exchanges, and most leading cloud and digital media platforms across its footprint, Interxion has created connectivity, cloud, content and finance hubs that foster growing customer communities of interest. For more information, please visit **www.interxion.com**

Data Centre services across Europe



www.interxion.com
customer.services@interxion.com

International Headquarters
Main: + 44 207 375 7070
Email: hq.info@interxion.com

European Customer Service Centre (ECSC)
Toll free Europe: + 800 00 999 222 / Toll free US: 185 55 999 222
Email: customer.services@interxion.com

Cofounder: Uptime Institute EMEA chapter. **Founding member:** European Data Centre Association. **Patron:** European Internet Exchange Association. **Member:** The Green Grid, with role on Advisory Council and Technical Committee. **Contributor:** EC Joint Research Centre on Sustainability. **Member:** EuroCloud.

Interxion is compliant with the internationally recognised ISO/IEC 27001 certification for Information Security Management and ISO 22301 for Business Continuity Management across all our European operations.

WP-CL-HQ-GUIDE-HQ-eng-4/18